(3)

J.D. Woodard
Executive Vice President

Southern Nuclear Operating Company, Inc.
40 Inverness Center Parkway
P.O. Box 1295
Birmingham, Alabama 35201

Tel 205.992.5086

'00 [illegible] 24 P2:07

SOUTHERN COMPANY
Energy to Serve Your World™

August 23, 2000

NEL-00-0214

Ms. Annette Vietti-Cook
Secretary of the Commission
U. S. Nuclear Regulatory Commission
ATTN: Rulemakings and Adjudications Staff
Washington, DC 20555-0001

DOCKET NUMBER
PROPOSED RULE PR 73
(65FR 36649)

Re: SECY-00-0063
(Staff Re-Evaluation of Power Reactor Physical Protection Regulations
and Position on a Definition of Radiological Sabotage)
as published in Federal Register Vol. 65, No. 112 dated June 2000

Ladies and Gentlemen:

Southern Nuclear Operating Company (SNC) endorses the comments on the subject SECY document contained in NEI's letter to the NRC on this topic. SNC is also submitting additional comments concerning the issuance of SECY-00-0063. Your efforts to re-evaluate current security regulations are greatly appreciated. It is hoped that changes made will be based upon facts consistent with logic used in other areas of nuclear power regulation and bring security regulations into the same framework of risk awareness.

The SECY discusses three comprehensive and interrelated issues:

1. Revision of 10 CFR 73.55 requirements.
2. Clarification of "Radiological Sabotage."
3. Industry-Developed Self-Assessment Program.

SNC comments to these issues are addressed in the Enclosure. Thank you for considering these comments.

Respectfully submitted,

J. D. Woodard

Enclosure

JGS/DWD/jdwsecy63.doc

Template= SECY-067

SECY-02

cc: Southern Nuclear Operating Company
Mr. J. B. Beasley, Jr., Vice President – Vogtle
Mr. D. N. Morey, Vice President – Farley
Mr. H. L. Sumner, Vice President – Hatch

Enclosure

Southern Nuclear Operating Company (SNC)
Comments concerning the issuance of SECY-00-0063
(Staff Re-Evaluation of Power Reactor Physical Protection Regulations) as published in
Federal Register Vol. 65, No. 112 dated June 2000

Federal Register Vol. 65, No. 112 requests public comment on three key issues contained in SECY 00-0063:

1. Revision of 10 CFR 73.55 Requirements.
2. Clarification of "Radiological Sabotage."
3. Industry-Developed Self-Assessment Program

SNC comments on these issues are as follows:

1. Revision of 10 CFR 73.55 Requirements.

The current security regulations commenced in the 1970s with little attention on security's protective strategy for defending against an overt attack and attempted radiological sabotage. As such, the industry has experienced a certain degree of "regulation by inspection," resulting in unwieldy and expensive security programs. Physical Security Plan commitments vary widely across the industry and perpetuate unnecessary and inconsistent requirements. Rulemaking that applies a risk-informed, performance-based approach is essential to properly focus program goals, resources, and outcomes. The key to a performance-based rule is a clear set of design criteria for which performance can be measured. These criteria should be consistent with other plant design criteria that must meet the radiological release requirements of 10 CFR Part 100. A process is also needed that clearly defines the adversary characteristics used in designing a security program to maintain a hard-target against attack.

While the current security regulations possess several noteworthy security elements (physical preventative methods, detection aids, contingency response capabilities, and security managerial systems), SNC perceives several problems with the current regulations. Specifically, they do not:

Use *credible threats* as a basis for a risk analysis/management process.
Give due consideration for the *deterrent* effect of existing security measures.
Recognize the inherent defense-in-depth concept of a reactor plant design.

Credible Threats

SNC believes that the Staff should consider developing a rational basis for defining the threat, and, therefore, avoid the continual intensification of adversary characteristics. Unfortunately, the Staff is currently contemplating several significant increases to the adversary characteristics, many which are beyond that used by the NRC's Operational Safeguards Response Evaluation (OSRE) process over the last 10 years.

Adversary capabilities used during OSRE drills have continued to escalate. With each new plant security upgrade, subsequent OSREs develop new defeat methods. This practice has required plants to implement ever increasing physical security measures, such as barriers, razor wire, and manned, hardened defensive positions.

Some of the weapons and capabilities contemplated in the draft adversary characteristics contradict NRC Statements of Consideration (32 FR 13446) where it indicates that commercial nuclear facilities were not expected to protect against such capabilities. Such an escalation may necessitate that site security personnel: (a) receive federal authority to possess equivalent weapons (e.g., automatic weapons), or (b) be protected by US/National Guard military forces.

Deterrence

The common characteristics of commercial power reactors (i.e., the "defense-in-depth" concept of reactor plant design) make the release of radioactivity due to malevolent acts of sabotage difficult. The massive containment structure and the procedures and systems for rapid shutdown provide some protection against the effects of enemy attacks and destructive acts, although that is not their specific purpose. One factor underlying the Commission's practices in this connection has been a recognition that reactor design features to protect against the full range of the modern arsenal of weapons are simply not practicable and that the defense and internal security capabilities of this country constitute of necessity, the basic "safeguards" with respect to possible hostile acts by an enemy of the United States.
This is reflected in 10 CFR 50.13, which states in part that:

"An applicant ... is not required to provide for design features or other measures for the specific purpose of protecting against the effects of (a) attacks and destructive acts, including sabotage, directed against the facility by an enemy of the United States..."

In most security contexts, the very existence of significant physical security measures dissuades potential malevolent acts. Additionally, postulated adversary capabilities appear to ignore the fundamental motivation of a terrorist as discussed in NUREG 0459 ("General Adversary Characteristics Summary Report"). Specifically, heavily defended targets, as in the case with all nuclear power plants, are avoided by terrorists. The focus needs to be on maintaining plants as *hard targets*, not on deploying countermeasures to every hypothetical terrorist capability.

While SNC recognizes the potential for a design basis threat attack and the hypothetical consequences, this potential threat is counterbalanced by inherent deterrence factors and the extremely low probability of such an attack. This reality should be incorporated into the Staff's current rulemaking process.

2. Clarification of "Radiological Sabotage."

An understanding of the level of protection to be provided to the public is fundamental to a performance based security rule. Additionally, the Commission's questions on "margin of safety" cannot be addressed adequately if the level of protection is not defined.

In other areas of nuclear plant design, the need to protect the public is ultimately addressed by preventing a radioactive release that exceeds 10 CFR Part 100 limits. There are a number of initiating events that are considered in the nuclear plant design and evaluation process. Attempted radiological sabotage should be considered as another initiating event, with the consequences analyzed on the same bases as the rest of the plant. The tools we have in place to perform accident

analysis and risk assessment were developed using the criteria of Part 100 and the postulated events that could challenge these limits.

To provide a safety margin, performance criteria must be set at some level below the level of successful radiological sabotage. In developing contingency response programs, significant core damage is currently being used as the performance criteria by both the NRC staff and the industry. It is considered an appropriate basis for future discussions on performance criteria.

For radiological sabotage to be successful, the malevolent activities have to lead to a large radiological release that exceeds 10 CFR Part 100 limits. The industry's understanding of radiological sabotage is supported by that expressed in NUREG 1178:[1]

"*Successful radiological sabotage results in doses in excess of those defined in 10 CFR 100. The 10 CFR 100 criteria are intended to serve as a benchmark for the analysis of major events, that is, those events that pose a potential health hazard (a significant release of radioactivity as a result of a major accident or radiological sabotage*)."

To provide an acceptable margin of safety, NUREG 1178 also states in its analysis assumptions that: *"Any transient or event that causes significant core damage will result in an attendant 10 CFR 100 release*." As such, "significant core damage" has been the basis for the industry's protection strategy and the NRC OSRE oversight program.

Critical Safety Functions:

The proposal inappropriately elevates protecting "critical safety functions" to the primary rule objective. This would create a significant problem in the development of a performance-based rule.

Currently, the industry's contingency response programs have been based on preventing significant core damage. As a development and evaluation tool, target sets were developed to identify functional structure, system, and component (SSC) groupings for performing particular functions. Since these target sets are only tools in the development of protection strategies for contingency response designed to protect the public by preventing significant core damage, these target sets in themselves should not become the key rule objective.

The current target sets developed under the OSRE process identify a range of equipment needed to perform certain functions. This has allowed development of defensive strategies that provide for better defense-in-depth responses to unexpected events. In developing target sets, key functions such as reactivity control, sources of makeup water, and reactor cooling must be considered. Identifying critical SSCs is a key tool in target set development, but should not become the ultimate goal for the security program.

In SRM-99-241, the Commission asked that, "In developing the rule, the staff should pay particular attention to the degree to which risk insights can be used to develop target sets, and to the integration of security inspections and performance indicators into the new oversight process. The rule should provide for flexibility in implementing its provisions, and, most importantly, it

[1] NUREG 1178 ("Vital Equipment/Area Guidelines Study," page 4-1

should not unnecessarily burden operational safety at nuclear power plants." It is unclear how these precepts would be fulfilled by critical safety functions as a criteria.

In May 2000 the industry provided in a public meeting draft rule language that provides a logical approach to meeting the overall performance objectives for physical protection of nuclear power plants. This approach consists of several layers. First is the access authorization program to assure the trustworthiness and reliability of personnel with unescorted access. Second is the barrier system and material search program. The third layer is a detection system to detect unauthorized attempts to enter the facility, and fourth is an assessment capability to evaluate the threat, if there is one. Fifth and finally is a contingency response capability to counter a threat. Target sets and contingency response performance criteria should only be elements of this fifth layer.

3. Industry Developed Self Assessment Program

The industry has developed a voluntary program, "Safeguards Performance Assessment" (SPA) which can be used to test and validate performance based criteria for the proposed rulemaking process. Before the Staff will endorse the industry developed SPA, they are maintaining that:

All nuclear sites commit to the SPA in their licensee security plan.
The industry replace "significant core damage" with "Critical Safety Functions" (CSF) for determining target set components.

SNC disagrees with the Staff's stipulation that sites must commit to the SPA in the security plan. First, the SPA is a "pilot" program. During its trial period, because it is a pilot program, it is likely to be revised several times to incorporate vital lessons learned. The industry must retain the flexibility to make these changes and then test them through the program. The NRC will still have the ability to inspect the activities described in the SPA by revising Attachment 3 to the Security Inspection Manual to address the SPA activities. Second, all sites making simultaneous security plan changes would be an administrative burden on the sites (and NRC) and would dilute resources that need to be dedicated to improving the program. Third, and most importantly, until SNC receives relief from current regulations that do not have any value added for physical security (viz. the generic 50.90 / exemption requests recently submitted by Texas Utilities and Commonwealth Edison), we view the addition of the SPA as a significant burden to existing security resources.

SNC also disagrees with use of CSF for determination of target set components as a replacement for the "significant core damage" criterion. As previously discussed, the latter ties back to the 10 CFR 100 dose limits and provides a proven and clearly understood criterion for threat analysis in common with other design basis events, as reflected in NUREG 1178, as opposed to the ill-defined and potentially overly prescriptive CSF approach.

Summary

In closing, SNC believes that substantial deterrence to direct armed assault by terrorist groups is inherent in the design features of nuclear power plants, and that adversary characteristics must be defined so that appropriate performance criteria can be established as part of the proposed rulemaking.